

Enterprise Open Systems User's Guide

September 2001



National Institutes of Health
Center for Information Technology
NIH Computer Center
Bethesda, Maryland 20892-5607

Publication No. CIT0001

Table of Contents

I INTRODUCTION

A. Preface	5
B. Overview of the EOS Systems	5
• CIT Services for EOS	5
• Summary of the EOS Systems	5

II GETTING STARTED

A. Establishing a New EOS Application	7
• Acquiring a CIT Account	7
• CIT's Role	7
<i>Application Listserv List—PROJ List</i>	
<i>CIT Contact</i>	
<i>ASR</i>	
<i>Application Name</i>	
• Application Participants	7
<i>Members</i>	
<i>Authorized Members</i>	
<i>Application Owners</i>	
• Application Responsibilities	8
• Terminating an Application	8
B. Application Service Request (ASR)	8
• One Place to Accomplish Everything	8
<i>Initiate Request</i>	
<i>Update Profile</i>	
<i>Manage Request Authorization</i>	
C. Information for New Users	9
• How To Log In and Log Out Using Secure Shell	9
<i>Important Issues to Remember</i>	
• Getting Online Help	9
<i>Unix Help</i>	
<i>Oracle Help</i>	
• Start Up Files	10
• E-Mail	10
• Editors	10
• Documentation	10
<i>Obtaining Copies</i>	

D. Operations Policies	11
• Communicating with CIT	11
• Operating Hours and Availability	11
<i>Hours</i>	
<i>System Maintenance</i>	
<i>Database Maintenance</i>	
<i>Upgrades</i>	
• Backup and Recovery	12
<i>Standard</i>	
<i>Non-Standard</i>	
• Importing Data to EOS Systems	12
• System Monitoring and Resource Management	12
<i>What We Monitor</i>	
<i>Acceptance of Monitoring</i>	
• Problems and Change Requests via ASR	13
• Increase in Resource Needs	13
<i>CIT Monitoring of Resources</i>	
<i>Requesting New Disk Space</i>	
• Application Software Installed on EOS	13
E. Security and Risk Management	14
• Security and System Access	14
• EOS System Security	14
• Individual Unix Accounts and Role-Based Unix Accounts	15
• Security Data Administration	15
• Passwords	15
<i>Expiration and Resetting</i>	
<i>Good Passwords</i>	
• Unix File Access Controls	16
F. Charging for the EOS Systems	16
• Billing	16
• Responsibilities of CIT and the Customer	16

III EOS SYSTEMS CONFIGURATION

A. Hardware and Software	17
• Servers	17
<i>Compaq/Digital AlphaServers</i>	
<i>Sun Servers</i>	
• Storage	17

A. Hardware and Software (Continued)

- Software 17
 - Operating Systems*
 - Database*
 - Connectivity*
 - Programming Languages*
 - Scripting Languages*
 - Web Servers*
- Software Supplied by the Customer 18

B. Applications 18

- CONNECT:Direct 18
- Web Servers 18
- Oracle Internet Application Server 19

C. Oracle RDBMS 19

- Basic Oracle Set Up 19
- Assistance to Database Users 19
- Training 20
- Sizing Considerations 20
- Server Options 20
 - Replication*
 - Intermedia*
- Version and Patch Levels 20
- Backups and Exports 20
- Documentation 20
- Definitions 21
 - Database Instance*
 - Executable Code*
 - Relational Database Management System (RDBMS)*
 - System Global Area (SGA)*

V APPENDIX

A. SecureCRT 22

- Welcome 22
- What Is SecureCRT? 23
- Connecting with the Connect Dialog 25
- Connecting with the Quick Connect Dialog 26
- Creating a New Session with Quick Connect 27
- Security Considerations 28
- Changing Session Options 29
- SSH1 Connection Settings 30
- SSH2 Connection Settings 32
- Overview of VCP 34



I INTRODUCTION

A. Preface

The *Enterprise Open Systems User's Guide* provides an overview of the Enterprise Open Systems (EOS), tells you how to get a new EOS application, and describes how to begin using your application when it is hosted in the EOS environment. Other information includes operations policies (e.g., security and risk management), charging, EOS systems configuration, and the products and services available to the applications hosted on EOS (e.g., Oracle RDBMS).

Information about the EOS systems is provided in two ways. Time-critical information is e-mailed directly to the Listserv list used for your EOS application. Planned upgrades, changes in policies, and new/revised EOS services/facilities are preannounced in our publication, *Interface*, and then incorporated into the *NIH Computer Center User's Guide*.

We are here to support you in fulfilling your organization's missions and goals. Please let us know how we can better serve you. If you have comments and questions, please call CIT's Technical Assistance and Support Center (TASC) at (301) 594-6248.

B. Overview of the EOS Systems

The Enterprise Open Systems (EOS) provides a stable software and data-repository environment for customer applications that run in a Unix-based environment. EOS provides hardware and software featuring powerful Compaq/Digital AlphaServers, Sun Enterprise servers, Oracle RDBMSs and related products, and complete Web capabilities. Use of the EOS is on a fee-for-service basis, with the costs charged to your CIT account.

- **CIT Services for EOS**

CIT staff provides a well-managed server environment suitable for critical Unix-based applications.

Hardware and software (e.g., secure-server platform, Oracle licenses) is acquired and maintained by CIT. The configuration is carefully tailored to the needs of the application.

CIT has long, broad experience in providing production facilities—including 365 day/year operation, physical plant maintenance, system security, disaster recovery procedures, and networking infrastructure. The CIT systems staff are experts in all aspects of operating and maintaining robust, secure system for hosting critical applications..

CIT staff can address your individual computing requirements and help tailor your applications to run efficiently in this environment. For more information, please contact the EOS team at (301) 496-5524.

- **Summary of the EOS Systems**

The NIH Computer Center's EOS platforms are Unix-based systems that provide extremely high performance with an outstanding price/performance ratio. The database servers are Compaq/Digital AlphaServer systems that are well known for their transaction processing capabilities—particularly in using its 64-bit architecture to complement Oracle database transactions. For more details, see "EOS Systems Configuration" (page 19).

Hardware

EOS database processing is based on high-end Compaq/Digital AlphaServers with readily expandable RAID and non-RAID disk storage. Midrange Compaq/Digital AlphaServers and Sun servers are also part of the EOS configuration and are available for multi-tier applications. These midrange servers have proven especially useful for hosting Web servers and middle-tier applications that access secure Oracle databases on the large, shared AlphaServers.

RDBMS

Recent versions of Oracle RDBMSs are available on the shared database servers. CIT staff will create and maintain Oracle instances for your application and provide the necessary licenses for direct access to the database. Oracle instance installation, maintenance, monitoring, and procurement are handled by CIT.

Monitoring

CIT staff monitors disk space, memory, and processor usage on all systems. We can help you decide when it's time to increase resources needed for your application.

Connectivity

CIT provides wide bandwidth network connections to and from EOS systems via SSH, scp, ODBC, Net8 (formerly SQL*Net), CONNECT:Direct, as well as with the Internet via http and https (SSL).

Flexibility

CIT can work with you to develop configurations of hardware and software that match your needs. As your requirements change (perhaps your development system is going production), you can add or subtract additional services and options. You only pay for what you currently use.

Security

Unix on the EOS Systems is installed and configured at the DoD C2 security level (approximately equivalent to DHHS Level 3 security). The NIH Computer Center is physically secure with card-key access. Facilities in the Computer Center—including the EOS systems—are monitored 24 hours a day, seven days a week. The computing environment has controlled humidity and temperature, as well as an uninterruptible power source. System data is backed up regularly, and the backup tapes are stored in a fireproof onsite vault and at a remote site. More information is available in "Security and Risk Management" (page 16).

II GETTING STARTED

Owners of applications that might benefit from using EOS systems are encouraged to contact CIT to discuss their application requirements. CIT will work with application owners to identify an appropriate hosting architecture – addressing the application’s processor, memory, storage, bandwidth, software, and security requirements. The hosting architecture and service/support level that is jointly selected will determine the monthly hosting costs.

A. Establishing a New EOS Application

To request a new EOS application, you can help us by providing us with information about your application. Please fill in and submit the “New EOS Application Request” at <http://datacenter.cit.nih.gov/eos/newapplication>. On receiving the information, an EOS consultant will contact you to discuss your needs in detail.

- **Acquiring a CIT Account**

The customer (application owner) must obtain a CIT account. The charges for using the EOS systems will be billed to this account. Go to <http://support.cit.nih.gov/accounts/> for details.

- **CIT’s Role**

Once the level of service has been agreed upon and the customer has a CIT account for billing, CIT will arrange for the following:

Application Listserv List—“PROJ List”

CIT will set up a list—“*application name*-PROJ@list.nih.gov”—to be used for e-mailing information on your application to all participants. We refer to this as the “PROJ list” for your application.

CIT Contact

CIT will assign an EOS consultant as your CIT “application coordinator.”

ASR

CIT will authorize you to use the Application Service Request (ASR) system for requesting changes in your level of service. See the Section on the ASR system (page 10).

Application Name

CIT will provide the application owner with the registered name assigned to the application, along with an ID and password for use in accessing the ASR system. ASR provides a mechanism for an owner to establish IDs and passwords for other application members.

- **Application Participants**

Your application will have several kinds of participants:

<i>Members</i>	anyone on the application Listserv list (“PROJ list”)
<i>Authorized Members</i>	can submit requests to the ASR system
<i>Application Owners</i>	has authority to obligate funds, and can delegate authority to an authorized member; adds and removes members from the ASR

- **Application Responsibilities**

All account and user management responsibilities can be accomplished online through the Application Service Request (ASR) program. (See the next section on ASR.)

- **Terminating an Application**

If an application is found to compromise the EOS operating environment, CIT may act to terminate the application. If termination becomes necessary, CIT will make every possible effort to work with the application's owner.

When there is a need to terminate the application, certain steps should be taken to ensure that the termination occurs in an efficient, orderly manner. Notification of termination by either party should:

- be received by the other party at least 60 days in advance
- be in written form, with the signature of the appropriate official, or submitted via ASR
- contain the reason for termination
- specify arrangements for disposition of data and associated resources

B. Application Service Request (ASR)

Everything related to your application is in the Application Service Request (ASR) system—including EOS resources used, people to contact, and users' names. The ASR system allows you to change, add, or subtract services. Use the ASR system for everything—for requesting new resources, updating telephone numbers, or finding a contact name and telephone number.

- **One Place to Accomplish Everything**

With just an ID and password, authorized people manage the application and communicate with CIT and others on the PROJ-list via ASR. When you access the ASR system, you will find three basic actions available:

- | | |
|---|---|
| <i>Initiate Request</i> | - request service for your application
(owner can create a co-owner with this authority) |
| <i>Update Profile</i> | - update the profile for this user
(e.g., change a password) |
| <i>Manage Request Authorizations</i> | - authorize other members (if authorized to do this) |

Once the request is submitted, notification is sent to the appropriate people, and tracking of the request is monitored to ensure timely response to your requests.

C. Information for New Users

- **How to Log In and Log Out Using Secure Shell**

Access to EOS systems is secured by the availability of secure shell (SSH). EOS systems accommodate both SSH1 and SSH2. In order to connect, use of a secure shell client is required. The DCSS client of choice is SecureCRT (Van Dyke Technologies, Inc.).

See the Appendix for configuration parameters and basic instructions for obtaining and using SecureCRT (page 24).

Important Issues to Remember

- 1) Your password will not appear on your terminal when you type it. Remember that Unix is case sensitive, so you must enter your username and password exactly.
 - 2) The first time you log on you will be forced to change your password. Simply follow the system's prompts.
 - 3) Changing your password at specific intervals is required. For more information on passwords, see Section E, "Security and Risk Management" (page 16).
 - 4) ***It is important not to leave a session unattended.*** When you are finished with the session, you can log out by typing the **logout** or **exit** command.
- **Getting On-Line Help**

Unix Help

The Unix **man** command gives on-screen information from the Unix "man" pages. These pages contain reference material designed to help you find information about a specific topic. The command **apropos** lets you search for "man" page entries based on a topic or keyword. Given a keyword, **apropos** lists all commands that are related to it. Unix manuals are available from the vendor.

Useful man commands include:

man man	get help about the man command
man ksh	get help about the Unix shell program ksh

Oracle Help

See "Assistance for Database Users" under Oracle RDBMS (page 21).

- **Start Up Files**

The default user shell on the EOS systems is **ksh** or the Korn shell. This is the environment provided for interactive users. The “*.profile*” file in the user’s home directory controls most environment variables. These can be modified to create a customized user environment. Please read the shell man page (**man ksh** or **man profile**) for more information.

- **E-Mail**

When an account is initially set up, a “*forward*” file is created in order to have your e-mail (received locally) forwarded to your preferred mail server. This file should contain a single line with your preferred e-mail address. This e-mail address may be changed to forward local mail to a different e-mail account. **Do not remove the “*forward*” file**, as this will cause the loss of your locally generated e-mail.

- **Editors**

The **vi** and **emacs** editors are available for full screen editing over an ssh connection. If you have X windows capabilities you can also use **dtpad**, **dxnotepad**, and **xedit**. See the respective on-line “man” pages for more information.

- **Documentation**

The following documentation is available to CIT registered users:

EOS User’s Guide

NIH Computer Center User’s Guide

- contains CIT’s policies and standards of service, as well as significant changes made to hardware and software on various platforms

OR

serves as an introduction to the OS/390 and other facilities offered by CIT

Batch Processing and Utilities at the NIH Computer Center

- includes information about CONTECT:Direct

Learning the UNIX Operating System

- general information about Unix

A Student’s Guide to Unix

Obtaining Copies

Copies of the *EOS User’s Guide* and the *NIH Computer Center User’s Guide* are available in printed or online format from CIT via the Web page **<http://publications.cit.nih.gov/>**. Look for the EOS guide under “General Documentation.” For hard copies of the Unix documentation, call the CIT help desk, TASC. Additional assistance is available from TASC at (301) 594-6248.

D. Operations Policies

General information on the NIH Computer Center's major systems and development facilities (including database systems) is available in the *NIH Computer Center User's Guide* (section 8). This *EOS User's Guide* contains additional information specific to the EOS systems.

- **Communicating with CIT**

All communication between established applications and CIT is accomplished via the ASR system. See also "Problems and Change Requests via ASR" (page 15).

- **Operating Hours and Availability**

Hours

The EOS systems operate 24-hours a day, seven days a week. For information, please contact TASC at (301) 594-6248—weekdays from 7:00 A.M. until 6:00 P.M.

System Maintenance

The production systems are reserved for maintenance activities between 5 A.M. and 8 A.M. on Mondays. PROJ lists are notified of maintenance that affects their applications.

Occasionally, major system upgrades may require a longer outage. Should this occur, notice will be sent at least seven-days in advance via the Listserv (PROJ) lists. The system may become unavailable at other times due to unforeseen events (e.g., power outage). If this occurs the CIT staff will make every effort to have the system available as soon as possible.

Database Maintenance

Database maintenance is coordinated with owners on an individual basis.

Upgrades

For events, such as hardware or operating system upgrades that might take longer than the scheduled maintenance hours, we will work with application contacts to lessen the effect of downtime on applications. Notification includes the date and duration of downtime, the reason for the change, and expected consequences.

Upgrades that customers wish to have installed should be requested via ASR. For more information, see the section "Problems and Change Requests via ASR" (page 15).

Major upgrades to facilities at the NIH Computer Center—including EOS—are announced in the periodical, *Interface*, available online at <http://datacenter.cit.nih.gov/interface>. To receive e-mail notice of new issues, join the Listserv list, "Interface," at <http://list.nih.gov/archives/interface.html>.

- **Backup and Recovery**

- Standard*

- Nightly incremental backups are done for all non-Oracle database instance data via the NIH Backup and Recovery Service (NBARS). Weekly “cold” backups of Oracle database files and certain Oracle files (e.g., config files and logs) are done so that the database is usually down for less than 10 minutes. The first weekly backup of the month is considered a “monthly” backup and is retained within TSM longer than weekly backups. Monthly Oracle backups also include both data and executable files.

- If requested by the application owner, full backups of Oracle exports can also be done nightly.

- Non-standard*

- Non-standard backup requests should be submitted using the ASR system. CIT will contact the application owner to work out the details.

- **Importing Data to the EOS Systems**

Please discuss all data import issues with CIT in advance, so that precautions can be taken to protect the integrity of the system and other users’ applications. In many cases, CIT may be able to recommend alternative methods that are compatible with our computing environment.

- **System Monitoring and Resource Management**

- What We Monitor*

- The CIT staff monitors system performance and availability throughout the day to verify that the systems are operational and Oracle databases are available. If problems occur, the staff is notified through NIH automatic monitoring systems.

- Whenever a potential problem is noticed, an investigation is launched. If the investigation reveals a problem that could affect Computer Center applications, the application contacts will be notified as soon as possible via the appropriate “PROJ list” or other expedient means.

- Acceptance of Monitoring*

- The following statement applies to all use of federal IT resources, including EOS:

THIS SYSTEM IS FOR THE USE OF AUTHORIZED USERS ONLY.
INDIVIDUALS USING THIS COMPUTER SYSTEM WITHOUT AUTHORITY OR
IN EXCESS OF THEIR AUTHORITY, ARE SUBJECT TO HAVING ALL OF
THEIR ACTIVITIES ON THIS SYSTEM MONITORED AND RECORDED BY
SYSTEMS PERSONNEL.

IN THE COURSE OF MONITORING INDIVIDUALS IMPROPERLY USING THIS
SYSTEM, OR IN THE COURSE OF SYSTEM MAINTENANCE, THE
ACTIVITIES OF AUTHORIZED USERS MAY ALSO BE MONITORED.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING AND IS ADVISED THAT IF SUCH MONITORING REVEALS POSSIBLE EVIDENCE OF CRIMINAL ACTIVITY, SYSTEM PERSONNEL MAY PROVIDE THE EVIDENCE OF SUCH MONITORING TO LAW ENFORCEMENT OFFICIALS.

NOTICE: U.S. Government Computer. Unauthorized Use Prohibited by Title 18, U.S.C.

Users acknowledge acceptance of these conditions through their continued use of the system.

- **Problems and Change Requests via ASR**

Please report all problems and change requests to CIT via ASR, *even in an emergency*. The ASR system will forward the request/report to all appropriate people (e.g., application owner and CIT). Using ASR also ensures tracking and monitoring.

The ASR system provides you with multiple dialog boxes, each containing options appropriate to your application. This ensures that you supply important information before you submit the ASR request.

Once the ASR report is submitted, e-mail is sent to the entire PROJ-list.

- **Increase in Resource Needs**

CIT Monitoring of Resources

CIT will proactively monitor application disk space, memory and CPU usage and suggest to the application contacts when it might be appropriate to have their allocated resources adjusted.

Requesting New Disk Space

Customers can request adjustments to disk space via ASR. If the request is for additional space—and that space is available—the change can be acted on within one week of receipt of the form.

Please provide at least 60 days advanced notice, when possible, since it may be necessary to acquire and install additional disk drives.

- **Application Software Installed on EOS**

If the customer wishes to have software installed on the EOS systems, the application owner should submit a change request via the ASR (see the next section on “Reporting Problems and Making Changes”). The application owner should work closely with CIT on such requests. CIT is responsible for ensuring the integrity of the EOS environment, and the CIT staff must first determine the impact of such software on the EOS environment.

If CIT determines that the software is compatible with the EOS environment, CIT will talk with the application contacts about the time required for installation and testing—which varies greatly and is

dependent upon both the software and the general circumstances. The application contacts should deliver software and documentation to the CIT application coordinator.

E. Security and Risk Management

The NIH Computer Center computing environment contains facilities that are robust and reliable. These facilities include:

- *7 X 24 system monitoring*
 - trained staff monitor system status around the clock
 - system experts on call at all times
- *uninterruptible power supply (UPS)*
 - fully “conditioned” power with extra duty battery backup
 - motor generators to take over from batteries to provide “never ending” power
- *normal physical and system security procedures, including*
 - annual audits by an independent auditing firm
 - security level verification appropriate for critical applications and highly sensitive data
- *climate control*
 - temperature and humidity control provide non-stressed hardware environment
- *central backup and recovery system*
 - nightly data backups
- *disaster recovery*
 - regular system-level backups to magnetic tapes, which are periodically moved offsite
- *data and access security*
 - forgotten Unix and Oracle DBA application password procedures
 - security violation investigations
- *rapid response to growing requirements*
 - procurement and supply systems are in place to permit rapid response to requests for additional services and resources
- *system software is maintained at current levels*
 - recent vendor upgrades and fixes are incorporated into system products and operating system

For questions about security issues, please contact the head of the CIT’s Application Services Branch at (301) 496-5524.

• Security and System Access

Due to access control policies in place for the EOS environment, CIT requires a static IP address for all users connecting via SSH and scp. This information is used to derive allowed-access lists. If an IP address needs to be added to the access list or if an address is no longer valid, these changes should be requested via ASR.

• EOS System Security

The EOS systems operate under Compaq Tru64 enhanced security, which is designed to meet or exceed C-2 level security (defined by the Department of Defense) and DHHS Level 3. The EOS systems provide password expiration and security checks, shadowed passwords, file access security, auditing and account resource limits.

In the interest of system security, the NIH Computer Center security officers reserve the right to check user passwords. If a password is “crackable,” the user and application contacts will be notified to change the password. If the password is not changed within the designated time period, the account will be locked.

- **Individual Unix Accounts and Role-Based Unix Accounts**

A unique, individual Unix ID must be obtained for each person requiring access to any of the EOS systems directly. This ID is to be restricted to the registered user and should never be shared with others. If there is a need for a Role Based Unix account or accounts, which perform a specific function requiring the effort of many individuals, each person should logon to the respective system with their unique ID and then change to the Role Based ID using the ‘su’ command.

It is mandatory for the security of an application that this policy be followed. This maintains the user-recognition chain of the security integrity requirements of the EOS C2 security environment by keeping the audit trail intact for each user accessing the system.

If there is any indication that the EOS security integrity is being compromised by the actions of a user or application (e.g., by ID sharing) CIT will take immediate action to terminate the suspect activity. Severe or repeated violations of security policy may require removal of an application or user from use of the EOS environment.

- **Security Data Administration**

Historical data is backed up “forever” for auditing purposes.

Checking password expirations is done weekly, with 14-day warning.

- **Passwords**

Passwords form the basis of account usage security.

Expiration and Resetting

- Passwords expire automatically after being in use for six months. They can be changed by using the Unix **passwd** command.
- You will not be able to reuse the same password for at least five generations.
- Any account that receives more than five consecutive login failures will be locked automatically by the system.

If your Unix account has been locked, or if you forget your password, please contact your application owner to request that your password be reset. The application owner must submit a password change request via ASR.

Good Passwords

These guidelines will make your password more difficult to crack. Most of these tips apply to other multi-user systems as well, and they are worth repeating here. Your password should:

- contain 6 to 10 characters
- contain at least one non-alphanumeric character. Any alphanumeric string, not just dictionary words, can be cracked
- differ from your previous password in at least 3 positions
- **not** have a digit at the end of the string of alphanumerics (e.g., acbdef8)
- **not** substitute l for I, 0 for o, or \$ for S in a word, without making other changes as well

To create a safe, easy-to-remember password, consider using a short phrase that is meaningful to you and includes punctuation (e.g., “home-again” or “home again”) or take the first letters and punctuation of a common phrase. For example, the phrase “I love work. I love Fridays” as a password would be **Ilw.IlF**. Examples of good passwords are

\$L1mERz G0ld;karD paS\$w3rD

Passwords should be easy to remember but hard to guess. They should not be your userid, social security number, birthday, spouse’s name, or other personal information that is easily obtainable. They should also never be written down or stored on line.

- **Unix File Access Controls**

The Unix file system defines permissions for the user of a file, members of the group, and everyone else. In a long directory listing (**ls -l**) the first column should appear something like

```
-rwxr-xr-x
```

This indicates read/write/execute permissions for the user, as well as read/execute for the groups and others. To eliminate general access to this file, use the **chmod** command as follows:

```
chmod go-rx filename
```

This will eliminate read/execute commands for the group and others, and the first column will look like

```
-rwx-----
```

F. Charging on the EOS Systems

The fees for the EOS systems can be composed of an initial start up cost, as well as monthly fees for service and storage at the NIH Computer Center. If you have questions about EOS systems charging, please call TASC at (301) 594-6248.

- **Billing**

Use of the EOS facilities is charged to the account specified for billing when the EOS application established. CIT bills the account monthly for use of the EOS systems.

- **Responsibilities of CIT and the Customer**

The conditions, responsibilities and costs governing the use of the EOS facility are mutually determined by CIT and the customer.

III EOS SYSTEMS CONFIGURATION

The EOS systems are constantly changing, as we upgrade facilities and adopt emerging technologies that will benefit our users. All major changes are announced in our technical newsletter, *Interface*, available on the Web at <http://datacenter.cit.nih.gov/interface>.

A. Hardware and Software

- **Servers**

- ***Compaq/Digital AlphaServer***

- Multiple Compaq/Digital AlphaServers—ranging in size from high performance GS series database servers to midrange application servers—all provide the processing power of 64-bit Alpha CPUs.

- ***Sun Servers***

- Multiple Sun midrange enterprise servers offering excellent performance for Web-enabled applications.

- **Storage**

The EOS systems have multiple, high capacity SCSI disks and are easily expandable. Most systems offer Redundant Arrays of Inexpensive Disks (RAID), a method of increasing the reliability of disk storage by mirroring, striping or storing parity information on the disks. This reduces the available storage space, but also decreases the likelihood of a catastrophic failure.

- **Software**

- ***Operating Systems***

- Tru64 UNIX
Sun Solaris

- ***Database***

- Oracle

- ***Connectivity***

- SSH Secure Shell
scp
Net8 (formerly SQL*NET)
CONNECT:Direct

- ***Programming Languages***

- C and C++
 - Perl
 - Standard Unix programming tools (e.g., sed, awk)

- ***Scripting Languages***

- Korn Shell (ksh)
 - Bourne Shell (sh)
 - Perl
 - Tcl/Tk

- ***Web Servers***

- Oracle Internet Application Server
 - Oracle middle-tier, Web-based server
 - Netscape Enterprise Server
 - Apache HTTP Server

- **Software Supplied by the Customer**

If the customer has supplied software for the EOS systems, the customer is responsible for supplying CIT with all updates to software, licenses and documentation. CIT staff will do the installation of all such software

B. Applications

The following applications are available on the EOS platform. Use of these applications should be discussed with CIT. In general, registration of users for these applications is handled by the application owner via submission of requests through the ASR system. Requests for other applications should be discussed with CIT.

- **CONNECT:Direct**

CONNECT:Direct is a product for transferring data—especially financial transactions—between different computer systems. CONNECT:Direct monitors the progress of the file transfer, similar to SENDFILE and RCVFILE programs (described in the CIT manual, *Batch Processing and Utilities at the NIH Computer Center*) but is easier to use. CONNECT:Direct monitors the progress of the file transfer.

CIT will work with the application owner to determine whether CONNECT:Direct can benefit your application.

- **Web Servers**

Netscape Enterprise Server (NES) and Apache HTTP Server are powerful Web servers for enterprises with large scale Web sites. These servers also enable rapid development of Web-based applications that can enhance communication, streamline processes and reduce costs.

- **Oracle Internet Application Server**

Oracle Internet Application Server allows for developing and deploying applications for the Web. Its scalable, distributed architecture and database integration provide a foundation for supporting business-critical applications accessed from Web browsers. This server is also a strategic platform for network application deployment that brings substantial savings over client/server-based applications through reduced complexity, better manageability, and simplified deployment.

Oracle Internet Application Server should be part of the service negotiated with CIT. Users need a Unix account to store application documents. The application owner can request a Unix account via ASR. Oracle userids and passwords are also obtained via ASR. For information on obtaining an oracle account, see “Oracle RDBMS: Getting Started” below.

C. Oracle RDBMS Server

Oracle is a relational database management system (RDBMS). The Oracle server is a high-performance database engine capable of handling large amounts of data, images and many concurrent users. It offers backup and recovery facilities and excellent security. The Oracle instances are installed, upgraded and maintained by the NIH Computer Center.

Oracle data is accessible interactively via client/server and Web connectivity or on-line connection. It can also be accessed by batch jobs. Online and batch application programming facilities allow programmers to embed SQL statements in C/C++. Client/server access allows an almost unlimited application development environment, including 4GL and Web environments. This capability allows users to create custom-tailored interfaces to Oracle data for their applications and to perform sophisticated data validation as it is entered.

An Oracle userid is required for the application’s database administrator (DBA), who can create and maintain additional userids. To register for individual userids, contact the application owner via ASR.

- **Basic Oracle Set Up**

An Oracle userid will be set up with the Oracle DBA role for the application’s database administrator (DBA), who can then create and maintain additional userids.

The basic service fee for Oracle RDBMS servers on the EOS systems includes installation and maintenance, upgrades and database systems support, as well as backups of Oracle system software and database files.

The basic fee also includes two dedicated Oracle instances—one for production and one for development/testing—and full public internet access for the application if desired.

- **Assistance for Database Users**

CIT provides a stable software and data-repository environment for enterprise-wide database and information systems at the NIH Computer Center. CIT assists organizations in implementing appropriate technologies to meet their centralized database and information processing needs, as well as keeps abreast of promising database and information processing technologies.

- **Support**

You can obtain information about Oracle documents and facilities at <http://silk.nih.gov/dbtech>. See also “Getting Online Help” and “Documentation” (pages 11 and 12). Additional information and support can be obtained from TASC at (301) 594-6248.

- **Training**

CIT’s computer training program offers database, Oracle, and Unix courses at no charge for CIT registered users. Information on these courses appears in the *NIH Computer Training* brochures. The list of courses and on-line registration are available at <http://training.cit.nih.gov>.

- **Sizing Considerations**

The application contacts should work with our staff to determine sizing requirements—including optimal memory utilization, system global area and disk utilization—for their database and application.

- **Server Options**

- **Replication**

Replication is a mechanism for supplying updated information across servers. Basic replication uses “read-only snapshots” to enforce a form of primary site replication. Such a “snapshot” is a full copy (or a subset) of a table that reflects a recent state of the master table. Replication is done to speed local queries and provide a degree of redundancy.

- **Intermedia**

This Oracle option is a text management solution that enables you to manage unstructured text information resources with the same security, scalability, and integrity as structured data that is stored in columns. With this option, you are able to build and deploy text-based applications with an SQL-like interface.

- **Version and Patch Levels**

CIT’s Oracle support staff will work with application contacts to coordinate changes to the database version levels and patches.

- **Backups and Exports**

One weekly cold backup and full export is included in the price of the your contract. Additional types and numbers of backups and exports can be negotiated with CIT. We encourage users to backup their data as needed.

- **Documentation**

Oracle manuals can be purchased from the vendor.

- **Definitions**

- ***Database Instance***

- A database instance is a collection of data files, as well as the software that manipulates it, and the memory associated with it. The system identifier (SID) is the name given to an instance.

- ***Executable Code***

- Executable code is a statements that performs actions specified by a program or a portion of a program.

- ***Relational Database Management System (RDBMS)***

- An RDBMS is a computer program for general-purpose data storage and retrieval that organizes data into tables consisting of one or more units of information (rows), each containing the same set of data items (columns). SQL (Structured Query Language) is used to manipulate data in an RDBMS. Oracle is an RDBMS.

- ***System Global Area (SGA)***

- The SGA is the memory used to store database information.

V APPENDIX

A. SecureCRT

The following pages are reproduced from SecureCRT online help.

Welcome

This help manual documents SecureCRT®, version 3.3. Please e-mail any questions you have to the following address:

SecureCRT-questions@vandyke.com

We will try to respond to inquiries within one to two business days.

If you have any comments or suggestions, please e-mail them to:

support@vandyke.com

For the latest information on SecureCRT and Van Dyke Technologies, Inc., check out our home page:

<http://www.vandyke.com>

Thank you!

The SecureCRT Product Team

[Copyright and trademark notices](#)

What is SecureCRT?

SecureCRT® is a 32-bit terminal emulator designed for Internet and intranet use with support for telnet, rlogin, and SSH® protocols. SSH is a secure protocol that replaces existing TCP/IP protocols such as telnet and rlogin. In order to establish secure connections, SSH must be supported by both the client and the server.

SecureCRT can be used for both secure and non-secure sessions. SecureCRT also has support for serial communications and modem dialing with the Windows® TAPI standard.

SecureCRT 3.3 requires Windows NT® 4.0, Windows 95/98, or Windows 2000.

For a list of new feature in SecureCRT, see [New in SecureCRT 3.3](#).

SecureCRT is highly customizable and easy to use. Remote sites can be easily accessed by simply entering a hostname. In addition, SecureCRT introduces the concept of a connection *session*. A session is a set of options and customized settings associated with or assigned to a connection to a remote machine. These settings and options are saved under a session name and allow the user to have different preferences for different hosts.

Security Features

- Support for both SSH1 and SSH2 protocols
- Port forwarding provides encryption for unsecure network traffic with protocols like SMTP, POP and IMAP
- Support for remote forwarding.
- X11 forwarding allows forwarding X Windows packets through the SSH session, which makes possible the encryption of the data between the client and server
- [VCP](#) command-line utility provides SFTP secure file transfers with SSH2
- Easy public key generation with the Key Generation Wizard
- Variable [SSH compression](#) allows session performance tuning on slow dial-up connections
- SSH1 security features include:
 - TIS, RSA, and Password authentication methods
 - DES, 3DES, RC4, and Blowfish encryption ciphers to ensure data privacy
 - RSA public-key identity file can be either global or session-specific
- SSH2™ security features include:
 - Password and public-key authentication methods
 - 3DES, RC4, and Twofish encryption ciphers to ensure data privacy
 - SHA1 and MD5 MACs (Message Authentication Codes) to ensure data integrity

General Features

- Named sessions allow the user to have different preferences for different hosts
- Simple mechanism for automating logons
- Telnet protocol support, including to a specific port
- Rlogin protocol support
- Serial (a.k.a. COM port) support
- Modem "sharing" with TAPI support
- Printing support: transparent printing; print selection and screen
- Easy installation

Advanced/Convenience Features

- Full Screen mode
- "Open URL" feature in pop-up menu (right mouse button)
- "Open Selection as URL" feature in pop-up menu (right mouse button)
- Keyboard accelerator (CTRL+Tab) to easily cycle between SecureCRT windows
- Support for use from the command line or web browsers
- Each session can be recorded in a log file
- Anti-idle support
- Searchable scrollbar buffer up to 32,000 lines
- User-defined number of savelines (scrollback)
- Support for Emacs Meta key
- Easy access to SecureCRT features through graphical toolbar
- User-defined word delimiter characters for word selection with double-click
- Optional chat window provides an editable type-ahead buffer

Emulation

- Quality VT100, VT102, VT220, Linux console, SCOANSI and ANSI emulation
- VT line drawing
- User-defined foreground and background colors for all eight combinations of text attributes (blink, underline, bold)
- Configurable number of rows and columns
- 80/132 column switching
- Ability to select separate fonts for both 80 and 132 column modes
- Double width and double height fonts (VT100, VT102, VT220)
- Optional ANSI color and customizable ANSI colors
- xterm extensions for mouse support and changing title bar
- 5 cursor styles and support for customizing cursor color
- National Replacement Characters sets (British, Dutch, Finnish, French, French Canadian, German, Italian, Norwegian/Danish, Spanish, Swedish, Swiss) --Requires remote host application support (VT100, VT102, VT220)

Keyboard mapping

- VT100, VT220 and SCOANSI keyboard emulation
- Support for user-defined custom keymaps
- Custom Keymap editor allows easy mapping of key combinations to:
 - Execute menu functions
 - Run scripts
 - Send string sequences
 - Call additional SecureCRT functions

Firewall support

- SOCKS version 4 and version 5 (telnet and SSH only)
- Generic telnet proxy firewall support

Scripting

- ActiveX scripting support allows use of multiple scripting languages including VBScript, JScript, PerlScript
- A simple expect/send dialog can be used to easily automate logon commands
- Support for file-based scripts:
 - Scripts can be run automatically at logon
 - Run a script at any time from the menu
 - Map a key combination to run a script using the Keymap editor
 - Run a script from the command line

File transfers

- ZModem file transfer (upload and download)
- Resume interrupted ZModem downloads
- Transfer list dialog allows selection of multiple files for ZModem upload
- XModem file transfer (upload and download)
- ASCII file transfer for upload and download
- [VCP](#), an SSH-based secure file transfer program, provides scriptable command-line transfers

Clipboard support

- Copy and paste, including an "Auto Copy" option
- Column select feature (ALT+Left click)

Connecting with the Connect Dialog

The **Connect** dialog can be accessed with the **Connect** button on the toolbar or by selecting the **Connect** menu item from the **File** menu. In order to connect to a remote machine using the **Connect** dialog, you must select a previously created session.

You can quickly create a new session by clicking on the [New Session](#) button, or by right-clicking on any folder in the **Connect** dialog and selecting **New Session** from the pop-up menu. If you would like to learn more about creating new sessions, see Chapter 4: [Creating and Editing Sessions](#).

To connect using a session you have already created, select the session and click on the **Connect** button. You can also connect to a session by double-clicking on the session name or by right-clicking on the session name and selecting **Connect** from the pop-up menu.

To display the **Connect** dialog automatically at startup, select the **Show dialog on startup** option found in the lower left corner of the **Connect** dialog.

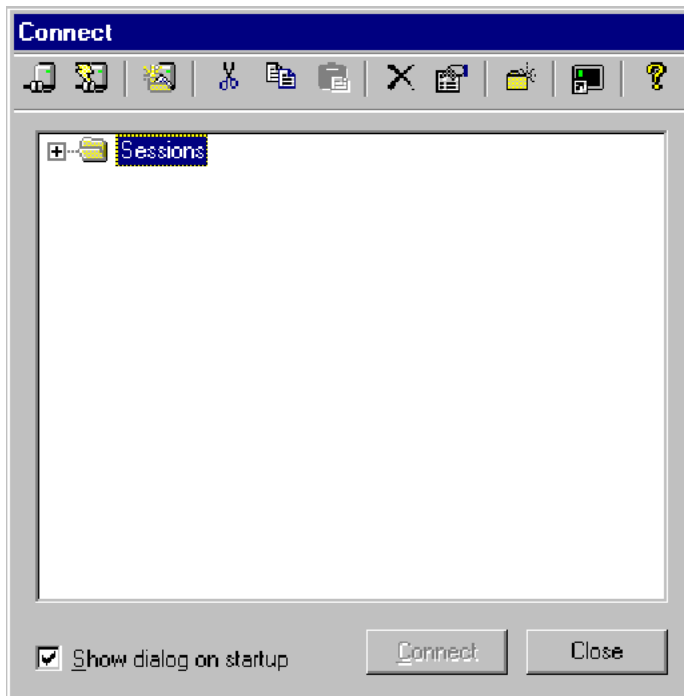


Figure 2.2 Connect Dialog

See also:

[Connecting with the Quick Connect Dialog](#)
[Sessions Overview](#)
[Creating a New Session with Quick Connect](#)
[Creating a New Session with Connect](#)

Connecting with the Quick Connect Dialog

By default, the **Quick Connect** dialog (see Figure 2.1 below) is shown when SecureCRT is started. If the **Quick Connect** dialog is not currently displayed, you can display it by clicking on the **Quick Connect** button , which is located on the main SecureCRT toolbar as well as the toolbar at the top of the **Connect** dialog. You can also display the **Quick Connect** dialog by opening the **File** menu and selecting the **Quick Connect** menu item. In the **Quick Connect** dialog, specify the protocol you will be using, the hostname or IP address, and any other information necessary to make the connection.

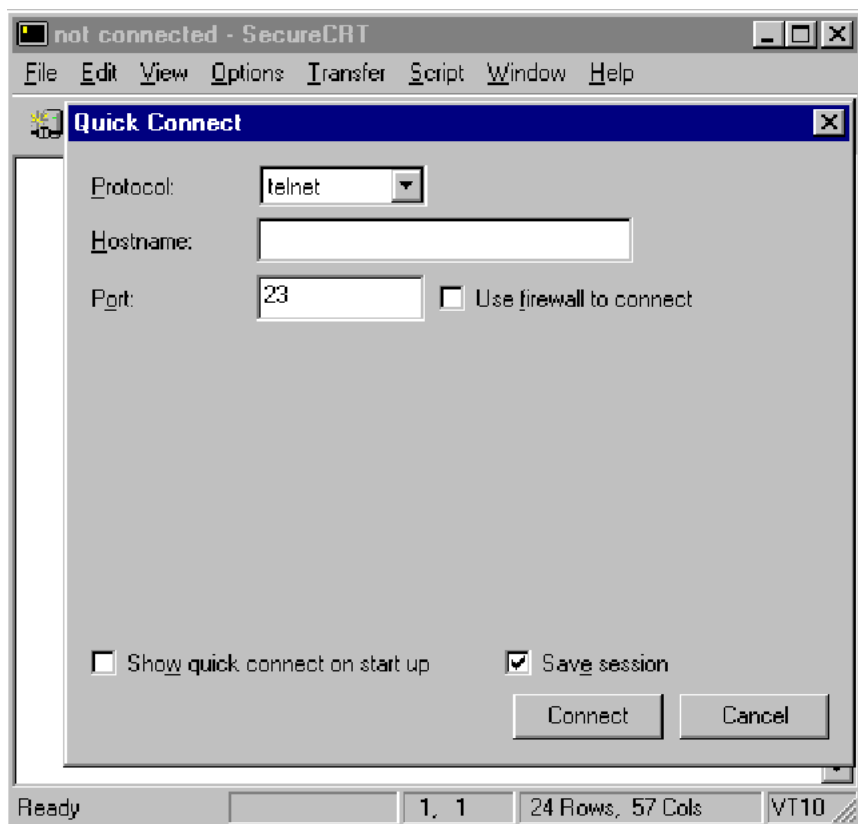


Figure 2.1 SecureCRT Main Window and Quick Connect Dialog (as shown at startup)

When finished entering the necessary settings for the connection, click on the **Connect** button and you will be connected to the specified host. If the **Save session** option is selected (this option is on by default), a session will be created and stored for future use under the name of the host or IP address you specified.

Note: You can customize SecureCRT to display the **Quick Connect** dialog on startup rather than the **Connect** dialog by selecting the **Show quick connect on start up** option located in the **Quick Connect** dialog.

See also:

[Connecting with the Connect Dialog](#)
[Sessions Overview](#)
[Creating a New Session with Quick Connect](#)
[Creating a New Session with Connect](#)

Creating a New Session with Quick Connect

The fastest way to create a new session and connect to the machine associated with it is to click on the **Quick Connect** button which is located on the toolbar at the top of the **Connect** dialog shown in [Figure 2.2](#). In the **Quick Connect** dialog ([Figure 4.1](#)), specify the [protocol](#) you will be using and all other information necessary to make the connection.

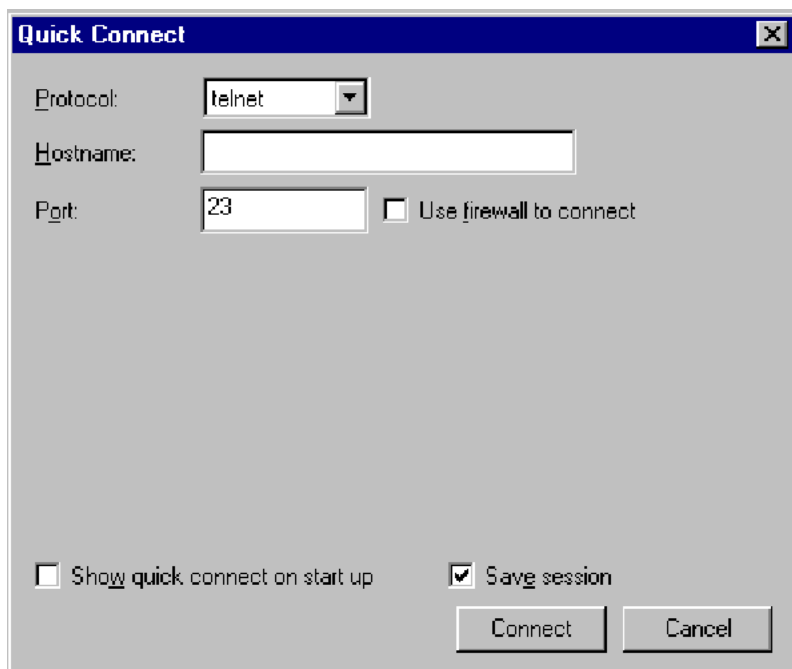
The image shows a 'Quick Connect' dialog box with a blue title bar. It contains three input fields: 'Protocol' with a dropdown menu showing 'telnet', 'Hostname' with an empty text box, and 'Port' with a text box showing '23'. To the right of the 'Port' field is a checkbox labeled 'Use firewall to connect'. At the bottom, there are two checkboxes: 'Show quick connect on start up' (unchecked) and 'Save session' (checked). Below these are two buttons: 'Connect' and 'Cancel'.

Figure 4.1 *Quick Connect Dialog*

When finished, click on the **Connect** button. If the **Save session** option is selected, a session will be created and stored for future use under the name of the hostname or IP address you specified, and you will be connected to the specified host.

Once you have created a session, you may wish to customize its behavior. For more information, see the topics in section 3.3, "Customizing Session Behavior".

Security Considerations

Session security depends on several factors, including whether the connection you are using to the host is a trusted connection. If it is not, consider whether private or confidential information will be sent and received. A telnet session will transmit user ID, password and other sensitive or private information in an easily readable format.

For maximum security, DO NOT put passwords in the SecureCRT **Script** dialog or script file. **Script** dialog information is stored in the SecureCRT configuration file, which may be accessed by other users depending on how open access is to the computer on which SecureCRT is installed.

Maximum security and privacy on the Internet and local networks requires the use of the Secure Shell Protocols (SSH1 and SSH2) supported in SecureCRT.

Note that although SecureCRT does support the telnet protocol, SecureCRT telnet sessions are not encrypted. Encrypted connections are achieved through the SSH1 and SSH2 protocols.

See also:

[SSH1 Connection Settings](#)
[Public-Key Authentication for SSH1](#)
[SSH2 Connection Settings](#)
[Public-Key Authentication for SSH2](#)
[Port forwarding with SSH](#)
[Overview of VCP](#)

Changing Session Options

Changing session options is done with the **Session Options** dialog. The **Session Options** dialog is accessed in a variety of ways.

If you are not currently connected with a session to a remote machine:

- Open the **Connect** dialog by clicking on the **Connect** button , or by opening the **File** menu and selecting the **Connect** menu item.
- Select the session listed in the **Connect** dialog that you would like to edit.
- Open the **Session Options** dialog by either clicking on the **Properties** button , or by right-clicking on the target session and selecting **Properties** from the pop-up menu. You can also open the **Session Options** dialog by selecting the target session and using the ALT+ENTER hot-key sequence.

If you are connected with a session to a remote machine and would like to edit the current open session:

- Open the **Session Options** dialog by either clicking on the **Properties** button , or by opening the **Options** menu and selecting the **Session Options...** menu item.

The **Session Options** dialog (Figure 4.3 below) is divided into two major sections: an options category tree view, and an options category panel. The options category tree view allows you to select the category of options you wish to change. The options category panel displays all the options associated with the category selected in the options category tree view. For example, in Figure 4.4-1 below, the **Connection** category is selected, and all of the options associated with the **Connection** category are displayed in the options category panel.

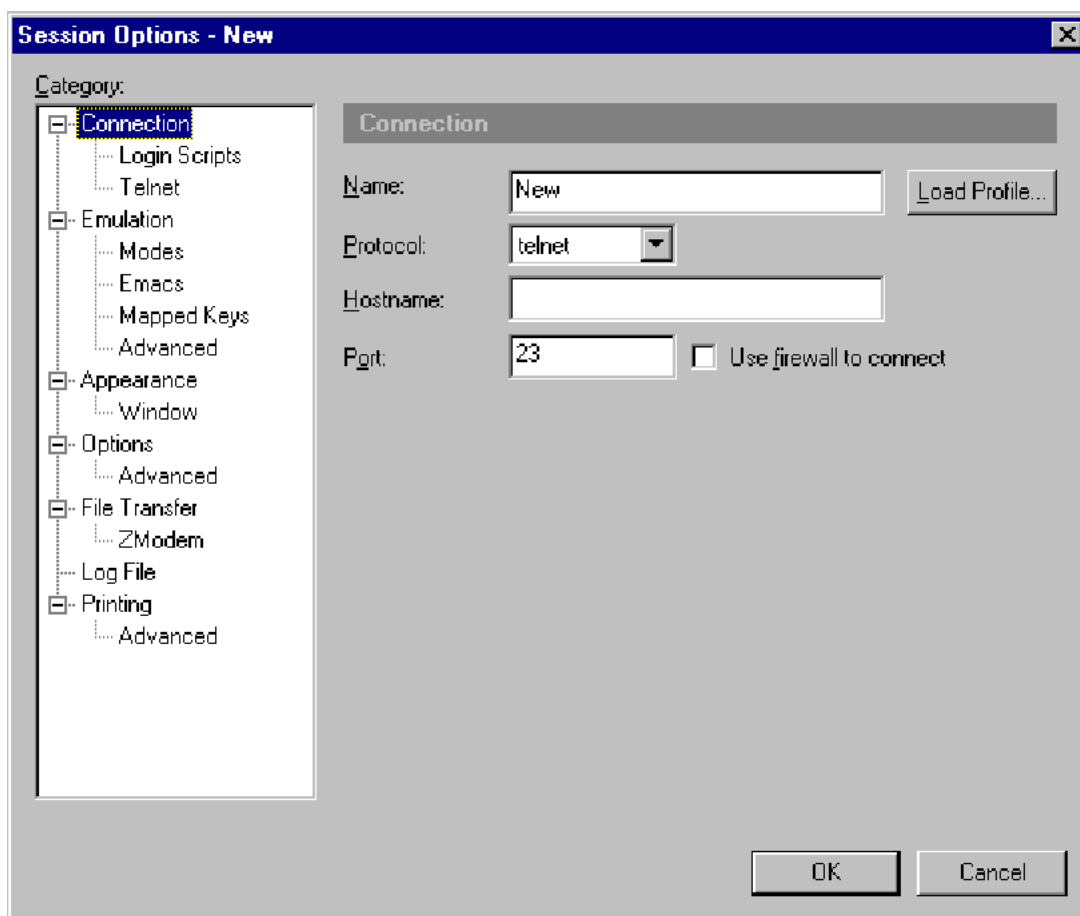


Figure 4.3 Session Options Dialog

See also:

[Saving Option Settings](#)

SSH1 Connection Settings

The SSH1 protocol is only available if selected when SecureCRT is installed.

SSH1 Overview

SSH1 provides secure communication over an unsecure channel by encrypting the data channel using the cipher algorithm selected for the session by the user.

WARNING: Setting cipher to None causes the data channel to be left unencrypted and offers no security.

The cipher selected must also be supported by the destination SSH1 server. An error will be reported during a connection attempt if the chosen cipher is not supported by the server.

Port forwarding is another feature based on SSH security. See [Port Forwarding with SSH](#) to learn more about encrypting connections for other applications (such as IMAP) that are not secure by default.

SSH1 connection settings include hostname, port, username, cipher, and authentication.

Hostname

The hostname or IP address of the remote machine that provides the SSH1 service.

Port

The port number of the SSH1 service on the remote machine. For SSH1, the default port is 22.

Use firewall to connect

If your connection involves a firewall, turning on (checking) this option causes the session to connect using the firewall settings configured in the [Global Options](#) dialog.

Username

The username used to log on to the remote machine.

Cipher

The encryption algorithm to use for data privacy. The default cipher is 3DES. DES, RC4 and Blowfish ciphers are also available for use with the SSH1 protocol. You may also set the cipher to None, which will effectively render your connection insecure. No encryption will occur if the cipher is set to None, and all data will be transmitted in plain text.

WARNING: Setting cipher to None causes the data channel to be left unencrypted and offers no security.

Cipher Speed Information

The DES and 3DES ciphers are very CPU intensive (slow). The RC4 and Blowfish ciphers are considerably less CPU intensive (faster).

Authentication

SecureCRT supports three types of authentication for connecting to SSH1 servers: password, RSA, and TIS.

Password authentication transmits the user's password to the server to authenticate the connection. The transmitted password is protected from network eavesdropping, due to the cipher encryption of the data channel. For this reason, some SSH1 servers reject the use of password authentication if the cipher is set to None.

RSA authentication uses a public/private key pair to authenticate the connection. The general mechanism behind RSA authentication is that the SSH1 server "challenges" the client to decrypt a message encoded using the user's public key stored on the server. Upon connecting, the SSH1 server generates a random value, encrypts the value using the user's public key and sends the encrypted challenge to the client. The client authenticates the connection by successfully decrypting the challenge using the user's private key. The security of the mechanism requires that no one but the owner have access to the private key. The private key is stored locally in an identity file. The first time you connect to an SSH1 server using RSA authentication, SecureCRT will prompt you for the location of this file. Also, prior to using RSA authentication, the public key must be made available to the SSH1 server.

Note: RSA authentication is only supported by the SSH1 protocol and is not an available option for the [SSH2](#) protocol. See [Public-Key Authentication for SSH1](#) to learn more about generating identity files and other setup issues.

TIS firewall authentication uses the TIS firewall server to provide a challenge phrase / response combination. SSH1 servers must be configured to offer TIS authentication.

See also:

[Key Terminology](#)

SSH1 Subcategory Settings

This panel allows you to turn on [compression](#) and set the [compression level](#).

Public Key Subcategory Settings

This panel allows you to set the [identity file](#) options.

Port Forwarding and X11 Subcategory Settings

This panel allows you to set the [port forwarding and X11](#) options.

SSH2 Connection Settings

The SSH2 protocol is only available if selected when SecureCRT is installed.

SSH2 Overview

SSH2 provides secure communication over an unsecure channel by encrypting the data channel using the cipher algorithm selected for the session by the user. The cipher selected must also be supported by the destination SSH2 server (an error will be reported during a connection attempt if the chosen cipher is not supported by the server). A cipher is used to encrypt network traffic between the local machine and the SSH2 server, thus providing data privacy.

Port forwarding is another feature based on SSH security. See [Port Forwarding with SSH](#) to learn more about encrypting connections for other applications (such as IMAP) that are not secure by default.

SSH2 connection settings include hostname, port, username, and authentication.

Hostname

The hostname or IP address of the remote machine that provides the SSH2 service.

Port

The port number of the SSH2 service on the remote machine. For SSH2, the default port is 22.

Use firewall to connect

If your connection involves a firewall, turning on (checking) this option causes the session to connect using the firewall settings configured in the [Global Options](#) dialog.

Username

The username used to log on to the remote machine.

Authentication

SecureCRT supports two authentication methods for connecting to SSH2 servers, and will attempt to connect using them in the order that you specify.

Password authentication transmits the user's password to the server to authenticate the connection. The transmitted password is protected from network eavesdropping, due to the cipher encryption of the data channel.

PublicKey authentication uses a public/private key pair to authenticate the connection. During the authentication process, the client and the server negotiate a public key to use for the connection. Once a public key has been determined, the client uses the corresponding private key to perform a signature operation over a unique connection identifier. This signature is then sent to the server for verification. If verification is successful, the client is given permission to connect to the server. The security of the mechanism requires that no one but the owner have access to the private key. The private key is stored locally in an identity file. Also, prior to using public-key authentication, the public key must be made available to the SSH2 server. For more information on generating private-public key pairs, see [Public-Key Authentication for SSH2](#).

See also:

[Key Terminology](#)

SSH2 Subcategory Settings

This panel allows you to turn on [compression](#) and set the [compression level](#), cipher, MAC, and SSH server.

Cipher

The encryption algorithm to use for data privacy. The ciphers provided for use with the SSH2 protocol in SecureCRT are AES, Twofish, Blowfish, 3DES, and RC4. You may also set the cipher to None, which will effectively render your connection insecure. No encryption will occur if the cipher is set to None, and all data will be transmitted in plain text.

WARNING: Setting cipher to None causes the data channel to be left unencrypted and offers no security.

SecureCRT will attempt to connect using the first selected cipher in the Cipher list and then, if not successful, work down the list trying each selected cipher. To reorder the list, select the cipher that you want to reposition and use the buttons to the right of the list to move the cipher up or down.

Cipher Speed Information

The 3DES cipher is very CPU intensive (slow). The RC4 and Twofish ciphers are considerably less CPU intensive (faster) than 3DES.

MAC (Message Authentication Code)

The SSH2 protocol provides increased security over SSH1 by means of a MAC (Message Authentication Codes) which ensures data integrity. Although specifying a MAC is optional, it is highly recommended that a MAC be specified in order to ensure data integrity. The MACs provided for use with the SSH2 protocol in SecureCRT are SHA1 and MD5.

WARNING: Data integrity cannot be ensured if MAC is set to None.

SecureCRT will attempt to connect using the first selected MAC in the MAC list and then, if not successful, work down the list trying each selected MAC. To reorder the list, select the MAC that you want to reposition and use the buttons to the right of the list to move the MAC up or down.

SSH Server

SSH2 server version. This value must match the SSH2 server version of the remote SSH2 server that you will be using. If you do not know the version of your SSH2 server, contact your system administrator. The default server version is Auto Detect. (Either the Auto Detect or Standard setting will work with Van Dyke Technologies VShell™ SSH2 server.)

Public Key Subcategory Settings

This panel allows you to set the [identity file](#) options.

Port Forwarding and X11 Subcategory Settings

This panel allows you to set the [port forwarding and X11](#) options.

Overview of VCP

SecureCRT supports the use of VCP (a simple file transfer program with SSH-based strong encryption) to securely copy files over the network. VCP uses SSH2 for data transfer providing users with the same authentication methods and security as SSH2. VCP is a commandline utility accessed from the Windows command prompt. VCP also uses the SecureCRT [host key](#) database.

Usage

The following is the format for VCP commands:

```
vcp [options] source [source ...] destination
```

VCP supports multiple sources. File source and destination are specified as follows:

```
[[user@]host[#port]:]file
```

File sources and destinations may contain a user, host and port specification to indicate that the file is to be copied to or from that host. Copies between two remote hosts are permitted. The following conditions apply:

- ▶ The `user@` argument is optional. If it is not specified, your Windows or network username will be used.
- ▶ The `host` argument is optional. If it is not specified, your current host is used but local-to-local transfers will not be permitted.
- ▶ The `#port` argument is optional. If it is not specified, the default port 22 will be used.
- ▶ The `file` argument can contain the wildcard characters `*` and `?`. These wildcard characters will be expanded by VCP. Only one `*` wildcard character is permitted in a file argument. Any wildcard characters to the right of the first `*` will not be expanded.

Options

The following table lists the command-line options that can be used with VCP commands.

<u>Option</u>	<u>Argument</u>	<u>Description</u>
-c	cipher	The cipher that the SSH2 server will use. Protocol strings or display strings are permitted.
-l	file	The identity file to use for public-key authentication. If no file is specified, VCP will use the SecureCRT Global Identity setting.
-m	mac	The MAC that the SSH2 server will use.
-q		Quiets (suppresses) screen output.
-r		Copies folders recursively (if you use this option, your source must be a folder).
-v		Displays verbose connection debug information.
-Z	n	The compression level (1-9).

Enterprise Open Systems User's Guide

Document Evaluation

Is the Manual:

	Yes	No
Clear?		
Well Organized?		
Complete?		
Accurate?		
Suitable for the beginner?		
Suitable for the advanced user?		

Comments:

Please give page references where appropriate.

If you wish a reply, include your name and mailing address.

Send to: The NIH Computer Center
Center for Information Technology
National Institutes of Health
Building 12A, Room 4011
Bethesda, MD 20892-5607

FAX to: (301) 496-6905

ICD:

Date Submitted:

Name (Optional):

September 2001